Document Control No. ECPN STP.2 10/10/96

Software Test Plan

(STP)

for the ECPN System

Version 1.0.6

10/10/96

Contract No. F19628-93-D-0019
CDRL Sequence No. B003

Prepared for:

Defense Information Systems Agency (DISA)
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Prepared by:

Inter-National Research Institute, Inc.
12350 Jefferson Avenue, Suite 380
Newport News, Virginia 23602

Document Control No. ECPN STP.2 10/10/96

Software Test Plan

(STP)

for the ECPN System

Version 1.0.6

10/10/96

Prepared for:

Defense Information Systems Agency (DISA)
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Prepared by:

Inter-National Research Institute, Inc.
12350 Jefferson Avenue, Suite 380
Newport News, Virginia 23602

Authenticated by _____ Approved by _____
(Contracting Agency) (Contractor)

Date _____ Date _____

The following trademarks and registered trademarks are mentioned in this document. Within the text of this document, the appropriate symbol for a trademark (™) or a registered trademark (®) appears after the first occurrence of each item.

Cleo is a registered trademark of Interface Systems, Incorporated.

HP is a trademark of Hewlett-Packard Company.

Kermit is a registered trademark of Henson Associates, Incorporated.

ORACLE is a registered trademark of ORACLE Corporation.

UNIX is a registered trademark in the Uninted States and other countries, licensed exclusively through X/Open Company Limited.

Table of Contents

This page has been intentionally left blank.

1.0 Scope

This section describes the scope of this Software Test Plan (STP). The standards set forth in Military Standard Software Development and Documentation (DOD-STD-498) and in the associated Data Item Description (DID) for a Software Test Plan were used as guides for this document with modifications made that would still preserve the intent. Sections that were not applicable were tailored out.

1.1 Identification

This STP applies to Version 1.0.6 of the Computer Software Configuration Item (CSCI) identified as the Electronic Commerce Processing Node (ECPN) of the Electronic Commerce/Electronic Data Interchange (EC/EDI) system.

1.2 System Overview

The EC/EDI system receives, processes, stores, and routes computer-to-computer messages for business transactions. Additionally, it monitors networks and alerts users of problem messages or communications trouble while providing an audit trail of system operations.

ECPN is being developed by Inter-National Research Institute (INRI) specifically for the EC/EDI system. The role of ECPN is to enhance the current EC/EDI Network Entry Point (NEP)/Gateway system. The fundamental objectives of this effort are to:

- Maintain rigorous accountability end-to-end within the NEP/Gateway processing, with no single point of failure that could cause loss or non-delivery of data.
- Automation of the processes required to place DISA EC/EDI into a high volume production environment; should include periodic automated reconciliation mechanisms to ensure that no deliveries are missed.
- Eliminate the UNIX® scripts and provide enhanced functionality in executable code.
- Enhance NEP/Gateway functionality by providing a transition from batch store/forward capability to single transaction mode.
- Implement basic ORACLE® RDBMS archival capability.
- Provide for backup archival, information retrieval, usage reporting and audit trails.
- Provide basic retransmission and recovery as well as status monitoring.
- Provide for automated notification of communication failure and restore and provide status monitoring.

1.3 Document Overview

The purpose of this STP is to describe the informal qualification testing being performed by INRI on ECPN. Note that Independent Verification and Validation (IV&V) testing is being performed by the Joint Interoperability Test Center (JITC).

This STP describes INRI's plans for ECPN qualification testing. It identifies the software test environment resources required for qualification testing and describes the individual tests that shall be performed during qualification testing. Qualification testing is designed to validate the ECPN against the requirements of the *Software Requirements Specification (SRS) for the ECPN CSCI.*

2.0 Referenced Documents

The following documents are referenced in this STP. In the event of a later version of a referenced document being issued, the later version shall supersede the referenced version.

- *Military Standard Software Development and Documentation* (MIL-STD-498), 5 December 1994.
- Data Item Description-*Software Test Plan* (DI-IPSC-81438), April 1989.
- *Software Requirements Specification (SRS) for ECPN CSCI*, February 1996.

3.0 Software Test Environment

All systems that will communicate with the ECPN must be included in the test environment. The test environment may be simulated or live. All required message transactions/lines and communication protocols must also be tested. Systems that will replicate these formats and protocols must be in place. For optimal testing, a live data feed with the real-world EC/EDI is highly recommended, but is not required.

The following subsections describe the software test environment for the ECPN. Included are descriptions of the plans for implementing and controlling the resources (software, hardware, and firmware) necessary to perform qualification testing.

3.1 Test Sites

As stated previously, INRI will perform informal qualification testing on ECPN and JITC will perform IV&V testing. The following subsections describe the software test environment at these sites.

3.1.1 Software Items

In addition to the ECPN, the Repeatable Performance Evaluator and Test (REPEAT) system will be used to perform the qualification testing activities. The REPEAT system serves the following purposes:

- Stores all data that is either sent or recorded, and provides the ability to examine and analyze messages.

- Provides the ability to continually retest using the same recorded data sets.

- Receives and transmits messages under the KERMIT® protocol, stores data, and makes it available for analysis.

3.1.2 **Required** Hardware and Firmware Items

The test environment will require at least three HP™ computers running ECPN. It will also require two modems: one modem for asynchronous testing and one modem for synchronous testing. An Annex communications server will be required for testing with the modems.

3.1.2.1 Test Equipment

A "CLEO® SYNCcable +" Asynch-to-Synch Converter will be required.

3.1.3 Other Materials

This section has been tailored out.

3.1.4 Proprietary Nature, Acquirer's Rights, and Licensing

This section has been tailored out.

4.0 Test Identification

This section identifies the informal qualification tests and the corresponding test requirements for each CSCI to which this STP applies. Since ECPN software is the only CSCI of the EC/EDI system being developed by INRI, only one set of qualification testing is identified. Appendix A contains a matrix relating the ECPN test classes described in this section to the system requirements.

4.1 ECPN

The following paragraphs describe the total scope of testing for the ECPN. This testing will follow a breakdown of ECPN capabilities according to functional areas. The functional areas are:

- Message Processing
- Log Management
- Alert Management
- Message Routing
- Comms Management and Comms Interfaces
- Database Management
- Translation
- Security
- Message Throughput

4.1.1 ECPN Test Levels

Informal qualification testing will be performed at these levels:

1. CSCI level, to evaluate compliance with CSCI requirements.

2. CSCI-to-CSCI integration level, to evaluate CSCI compliance with external interface requirements to CSCIs.

3. CSCI-to-HWCI integration level, to evaluate CSCI compliance with external interface requirements to HWCIs.

4.1.2 ECPN Test Classes

The following types of formal qualification tests will be executed:

1. Maximum capacity tests that examine the maximum data exchange load of ECPN to the failure point. The maximum size of a file is restricted to 10 megabytes (MB) for the test environment. The maximum number of message logs is restricted to 10,000 logs. The maximum number of messages in each log is restricted to 50,000 messages. The maximum number of alerts in the alert log is restricted to 2,500 alerts.

2. Data reception and transmission load tests to the failure point. The KERMIT protocol will be tested for proper operation within its design capability of 50 to 115,200 bits per second. The CLEO protocol will be tested for proper operation within its design capability of 1,200 to 14,400 bits per second. FTP and EMAIL protocols will be tested at the maximum rate possible for available network hardware.

3. Erroneous input tests. These tests verify the capability of the error-checking routines to trap errors entered by operators or errors in message transfers without causing system failure.

4. Stress tests that necessitate constant message processing for an extended period of time to determine Mean Time Between Failure (MTBF).

5. Performance tests that examine proper responses to all test inputs. These tests attempt to determine any limitations to the operation of the system and identify the conditions under which the system may become unusable.

6. Security tests that verify the capability of the system to control access to programs, data, operating system components, and devices, through the use of standard UNIX network security procedures.

4.1.3 General ECPN Test Requirements

Each formal qualification test will meet the following general test requirements:

1. The ECPN will be tested using average inputs, extreme inputs, and erroneous inputs. This form of testing shall occur under normal circumstances. ECPN performance will be determined by measuring message processing rates and response times.

2. The ECPN will be tested for error detection and proper error recovery, including appropriate error messages. This form of testing will occur when invalid messages are being received, and invalid user entries are being made.

3. The ECPN will be stressed with heavy loads of data for an extended period of time. This form of testing will occur at each integration to ensure that the system is working properly and will entail incremental increases in load until the system fails to work properly.

4. The ECPN will be tested to verify that adequate security measures are in place and to identify unauthorized system entry points.

4.2 Planned Tests

4.2.1 ECPN Test Definitions

The following subparagraphs define the tests used in each ECPN functional area identified in Section 4.1.

4.2.1.1 Message Processing Test

1. Test Objectives

   - Verify ability to process various types of message / line types containing various transaction types.
   - Verify ability to process / transmit 50,000+ messages.
   - Verify that all correctly formatted messages are processed.
   - Verify that incorrectly formatted messages fail.

2. Special requirements - Simulated or live data representing all of these required message transaction types must be available: 850, 843, 840, 838, 836, 997, 810, 870, 869, 820, 832, 855, 860, 865, 824, 864 and formats based on the basic format line types used in message comms (i.e., ISA, GS, ST, etc.). Downline systems capable of receiving outgoing traffic from all channels must be available. Each downline system must provide sufficient information on received traffic to allow investigation of the order of received messages and time of receipt.

3. Test level - CSCI, CSCI to CSCI

4. Test class - Data reception, performance, stress

4.2.1.2 Log Management Test

1. Test Objectives

   - Verify correct message parsing / storage to incoming / outgoing logs.
   - Verify ability to create 10,000 incoming / outgoing logs.
   - Verify ability to delete single / multiple logs.
   - Verify ability to edit incoming / outgoing logs.
   - Verify ability to clean single / multiple incoming / outgoing logs.
   - Verify ability to view incoming / outgoing logs.

- Verify ability to exit incoming/outgoing log manager.
- Ensure ability to manipulate messages in logs.
- Verify ability to archive/restore messages.
- Verify ability to archive/restore logs.
- Verify automatic archiving of messages that will be lost due to log wrapping.

2. Special requirements - None
3. Test level - CSCI, CSCI to CSCI
4. Test class - Data reception, performance, maximum capacity

4.2.1.3 Alert Management Test

1. Test objectives - The objectives of this test are as follows:
   - Verify all alert types (9) can be generated.
   - Verify function stability when maximum number of alerts (2500) is reached.
   - Verify ability to dismiss alerts (single, multiple).
   - Ensure ability to add notification(s) for specific alerts.
   - Ensure ability to edit existing notification.
   - Ensure ability to delete existing notification(s).
   - Verify that duplicate actions cannot be assigned to a single notification.
   - Verify that only active notification matches are acted upon.
   - Verify that all active alert notifications are generated.
   - Verify that action(s) are correctly performed.
2. Special requirements - All notification vehicles must be tested (email, beeper, window).
3. Test level - CSCI, CSCI to CSCI
4. Test class - Maximum capacity, erroneous input, performance

4.2.1.4 Message Routing Test

1. Test objectives:

   - Verify ability to create a routing criteria.
   - Verify ability to edit a routing criteria.
   - Verify that all valid source and destination channels appear as choices in their respective selection boxes.
   - Verify ability to delete routing criteria.
   - Verify correct message routing according to routing criteria.
   - Verify that only active routing matches are acted upon.
   - Verify ability to archive / restore the routing table.

2. Special requirements - All message formats must be tested.

3. Test level - CSCI, CSCI to CSCI

4. Test class - Performance, stress

4.2.1.5 Comms Management and Comms Interfaces Test

1. Test objectives:

   - Verify ability to configure all comms interfaces: CLEO, KERMIT, ZMODEM, EMAIL, and FTP.
   - Verify successful connectivity with all required external interfaces.
   - Verify ability to edit all interfaces.
   - Verify ability to delete interface(s).
   - Verify proper operation of each interface individually using the minimum and maximum baud rate for that interface.
   - Verify proper operation of each interface individually using the minimum and maximum message sizes.
   - Verify proper operation of all interfaces simultaneously using the minimum and maximum message sizes, and maximum baud rate for each interface.

- Verify proper operation of the system using the following simultaneous interfaces: 38 FTP, 25 KERMIT, 11 CLEO, and 3 EMAIL channels.

2. Special requirements - All external comms interfaces (CLEO, KERMIT, ZMODEM, EMAIL, and FTP) must be available for the tests.

3. Test level - CSCI to HWCI

4. Test class - Data reception and transmission load, performance, stress

4.2.1.6 Database Management Test

1. Test objectives:

   - Verify ability to configure and manipulate network table.
   - Verify ability to configure and manipulate email address table.
   - Verify ability to configure and manipulate segment terminator database.
   - Verify ability to configure and manipulate remote user database.
   - Ensure correct usage / verification of all database entries.
   - Verify ability to archive / restore various database tables.
   - Verify ability to replicate database from one system to another.

2. Special requirements - None

3. Test level - CSCI

4. Test class - Erroneous input, maximum capacity

4.2.1.7 Translation Test

1. Test objective:

   Verify ability to translate X12 format messages into various User Defined Format (UDF) messages.

2. Special requirements - None

3. Test level - CSCI

4. Test class - Erroneous input, performance

4.2.1.8 Security Test

1. Test objective:

   Verify ability to ensure the integrity of programs, data, operating system components, device access, and user identity through the use of standard UNIX network security procedures.

2. Special requirements - None

3. Test level - CSCI, CSCI-to-CSCI

4. Test class - Security, erroneous input

4.2.1.9 Message Throughtput Test

1. Test objective:

   Determine the throughput of the ECPN software under various conditions using the ftp interfaces to load the system. (Ftp was chosen for its higher transfer rate.)

   Verify the ability to handle increasing message flow with zero message loss.

2. Special requirements - None

3. Test level - CSCI, CSCI-to-CSCI

4. Test class - Maximum capacity, data reception/transmission load test, and performance test.

4.2.1.9.1 First Throughput Test Case

The purpose of this test case is to determine the throughput of the ECPN software using the ftp interfaces. The following three files, representing various combinations of ISA, GS, and ST segments, have been selected for use in this test:

Filename	SIZE IN BYTES	# ISA	# GS	# ST
test_356k	356,074	66	66	66
test_635k	635,018	1	1	392
test_13p5meg	13,538,262	1	5	5

The configuration shown below will be used to test the ability of the ECPN to handle various loads without error, and will determine throughput in average number of transactions (STs) per minute. No modification to segment terminators will be required. To simplify data injection and collection, this test will focus on loading the NEP with data from a single VAN for routing to a single Gateway.

The first test case will be conducted as follows:

1. Configure ftp interfaces with a 2-minute cycle-time between the VAN and the NEP and between the NEP and the Gateway.

2. Configure the X12 Routing Table to route all incoming messages from the VAN out to the Gateway.

3. Clean all incoming and outgoing logs.

4. Turn OFF both ftp interfaces configured in Step 2.

5. Place a copy of the first file into the proper OUT directory of the VAN.

6. Turn ON both ftp interfaces configured in Step 2.

7. Allow the file to be processed and forwarded.

8. Note the Time of Receipt (TOR) in the incoming log, and verify that the number of messages (ISA, GS, and ST) matches the predetermined value.

9. Note the Time of Transmission (TOT) in the outgoing log, and verify that the number of messages (ISA only) matches the value in the incoming log.

10. Subtract TOR from TOT to obtain throughput time.

11. Verify that the size of the file placed in the GATEWAY IN directory matches input file size, then delete the file.

12. Repeat Steps 3 through 11 until each file has been checked three times.

13. Repeat Steps 3 through 12 for the next two files.

14. Clean all logs.

15. Turn OFF both ftp interfaces.

16. Place one copy of all three files into the OUT directory of the VAN.

17. Turn ON both ftp interfaces.

18. Allow the files to be processed and forwarded.

19. Repeat Steps 9 through 12.

20. Clean all logs.

21. Turn OFF both ftp interfaces.

22. Place two copies of all three files into the OUT directory of the VAN, using unique names for the copies and repeat Steps 7 through 12.

23. Place three copies of all three files into the OUT directory of the VAN, using unique names for the copies and repeat Steps 7 through 12.

4.2.1.9.2 Second Throughput Test Case

The configuration shown below will be used to test the ability of the ECPN to handle various loads without error and will determine throughput in average number of transactions (STs) per minute. No modification to segment terminators will be required. This test will focus on loading the NEP with data from a multiple VANs for routing to a single Gateway. The number of VANs will be increased incrementally (to a maximum of ten).
The second test case will be conducted as follows:

1. Configure all ftp interfaces with a 2-minute cycle-time between the VANs and the NEP and between the NEP and the Gateway.

2. Configure the X12 Routing Table to route all incoming messages from the VANs out to the Gateway.

3. Clean all incoming and outgoing logs.

4. Turn OFF all ftp interfaces configured in Step 2.

5. Place one copy of all three files into the OUT directory of each VAN.

6. Turn ON all ftp interfaces.

7. Allow the files to be processed and forwarded.

8. Note the Time of Receipt (TOR) in the incoming log, and verify that the number of messages (ISA, GS, and ST) matches the predetermined value.

9. Note the Time of Transmission (TOT) in the outgoing log, and verify that the number of messages (ISA only) matches the value in the incoming log.

10. Subtract TOR from TOT to obtain throughput time.

11. Verify that the size of the files placed in the GATEWAY IN directory matches input file size, then delete the files.

12. Turn OFF all ftp interfaces.

13. Clean all incoming and outgoing logs.

14. Place two copies of all three files into the OUT directory of each VAN, using unique names for the copies and repeat Steps 6 through 13.

15. Place three copies of all three files into the OUT directory of each VAN, using unique names for the copies and repeat Steps 6 through 13.

4.2.1.9.3 Third Throughput Test Case

The configuration shown for the second test case will be used in this test also. The purpose is to verify the ability of the ECPN to handle various loads without error and determine throughput in average number of transactions (STs) per minute while requiring modification to segment terminators. This test will focus on loading the NEP with data from a multiple VANs for routing to a single Gateway.

The third test case will be conducted as follows:

1. Configure all ftp interfaces with a 2-minute cycle-time between the VANs and the NEP and between the NEP and the Gateway.

2. Configure the X12 Routing Table to route all incoming messages from the VANs out to the Gateway.

3. Configure the Seg Term DB to modify all transactions from the VANs to the NEP.

4. Clean all incoming and outgoing logs.

5. Turn OFF all ftp interfaces configured in Step 2.

6. Place one copy of all three files into the OUT directory of each VAN.

7. Turn ON all ftp interfaces.

8. Allow the files to be processed and forwarded.

9. Note the Time of Receipt (TOR) in the incoming log, and verify that the number of messages (ISA, GS, and ST) matches the predetermined value.

10. Note the Time of Transmission (TOT) in the outgoing log, and verify that the number of messages (ISA only) matches the value in the incoming log.

11. Subtract TOR from TOT to obtain throughput time.

12. Verify that the size of the files placed in the GATEWAY IN directory matches input file size, then delete the files.

13. Turn OFF all ftp interfaces.

14. Clean all incoming and outgoing logs.

15. Place two copies of all three files into the OUT directory of each VAN, using unique names for the copies and repeat Steps 6 through 13.

16. Place three copies of all three files into the OUT directory of each VAN, using unique names for the copies and repeat Steps 6 through 13.

5.0 Notes

The following acronyms and abbreviations are used in this document:

CSCI	Computer Software Configuration Item
DID	Data Item Description
DISA	Defense Information Systems Agency
EC/EDI	Electronic Commerce/Electronic Data Interchange
ECPN	Electronic Commerce Processing Node
email	Electronic Mail
FTP	File Transfer Protocol
HP	Hewlett-Packard
HWCI	Hardware Configuration Item
INRI	Inter-National Research Institute
IV&V	Independent Verification and Validation
JITC	Joint Interoperability Test Center
MB	Megabyte
MTBF	Mean Time Between Failure
NEP	Network Entry Point
REPEAT	Repeatable Performance Evaluator and Test System
SRS	Software Requirements Specification
STP	Software Test Plan
TOR	Time of Receipt
TOT	Time of Transmit
UDF	User Defined Format
VAN	Value Added Network

Appendix A Requirements Traceability

This appendix provides traceability from each test class identified in Section 4.1.2 of this plan to the requirements described in Section 3.2 of the Software Requirements Specification (SRS) for the ECPN CSCI.

The test classes identified in this plan are as follows:

Test 1: Message Processing Test
Test 2: Log Management Test
Test 3: Alert Management Test
Test 4: Message Routing Test
Test 5: Comms Management and Comms Interfaces Test
Test 6: Database Management Test
Test 7: Translation Test
Test 8: Security Test
Test 9: Message Throughput Test

Req. No.	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6	Test 7	**Test 8**	**Test 9**
001					X				
002					X				X
003					X				
004					X				
005					X				
006	X	X		X	X				
007					X				
008						X			
009	X	X		X	X	X			X
010								X	
011					X				
012	X		X						
013					X				
014			X						
015			X						
016			X						
017	X	X							
018		X							
019						X			
020	X								
021		X				X			
022					X				
023				X					
024								X	
025		X							
026						X			
027	X	X	X						
028				X					

029	X								